REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Objection to Specification

The specification has been amended by changing "EXOR" to –XOR– on pages 5-6, as required in item 2 on page 2 of the Official Action.

In addition, the specification has been revised to place the application in proper U.S. format by adding appropriate headers.

Because the changes are all formal in nature, it is respectfully submitted that the changes do not involve new matter.

2. Objection to Claims

This objection has been addressed by amending claims 3 and 9 to recite –XOR– rather than "EXOR," and by deleting the word "undisguised" in claims 1 and 9, as required in item 3 on page 2 of the Official Action.

3. Rejection of Claims 1-18 Under 35 USC §101

This rejection is respectfully traversed on the grounds that original claim 1 positively recited a **data carrier** with a **semi-conductor chip** including a **memory** containing an **operating program** able to execute the steps of disguising an operation and input data. A **data carrier** with a **chip** and **memory** is a tangible, real word object, and a data carrier capable of disguising operations and input data, *i.e.*, that protects data and therefore provides increased security, is clearly a practical application.

Card security is a major technical problem in the real world, and there are numerous patents directed to card security, most of which involve use of mathematical algorithms. This

is true of the two patents cited by the Examiner, both of which recite calculating methods, which is an even more mathematical way of reciting card security than the current positive recitation of a "*data carrier having a semiconductor chip with at least one memory containing an operating program. . . .*" An improved **data carrier** is far more physical than the methods recited in the prior patents, and no less statutory than an improved widget or mousetrap. The invention involves a concrete technical solution to the problem of protecting secret data present in the chip of a data carrier from unauthorized access, and therefore cannot be regarded as a pure mathematical method or algorithm..

Even though an improved "data carrier" is believed to be clearly statutory, **claims 1 and 9** have been amended to explicitly recite that the disguising operations carried out by the operating program are for the purpose of preventing a potential attacker from inferring secret information about the semiconductor chip (*e.g.*, the structure of the chip) by intercepting signal patterns. This is accomplished by adding false, irrelevant operations to any security-relevant operations carried out by the chip, making it more difficult to carry out statistical analysis of the actual security-relevant operations, as explained in the **paragraph bridging pages 1 and 2 of the original specification**. The invention involves disguising input data in such a way that instead of performing an operation on input data (which when repeated enables analysis of chip structure based on generated signal patterns), the input data is modified (disguised) in such a way that the data carrier can perform <u>different</u>, randomly disguised versions of the operation *and still obtain the same result as if the original, undisguised operation had been performed on the original undisguised data.* <u>In effect, the invention adds a random element to the security-relevant operations so that each time the operation is repeated, the data stream looks different to an outside observer</u>.

It is respectfully submitted that this the modification of data and operations so as to protect secret information about a chip on a data carrier is not a matter of pure mathematics, but an extremely useful technical innovation with immediate practical application in the field of data

carrier security, and therefore withdrawal of the rejection of claims 1-18 under 35 USC §101 is respectfully requested.

5. Rejection of Claims 1, 2, 4, 6, 7, 8, and 18 Under 35 USC §102(b) in view of U.S. Patent No. 5,153,581 (Saada)

This rejection is respectfully traversed on the grounds that the Saada patent does not disclose or suggest a data carrier having a semiconductor chip with a memory and operating program that:

a. disguises an operation before execution, and

b. executes the operation with disguised input data in such a way that the result of the execution of the disguised operation with the disguised data is the same as if the undisguised operation (*i.e.*, the original operation before being undisguised) had been executed with the undisguised data, as recited in claims 1 and 9.

In addition, it is respectfully submitted the Saada patent does not disclose or suggest the random disguising recited in claims 2 and 10 or the specific operations recited in the remaining claims, including the use of *two disguised operations* (claims 5 and 13), and the use of two random number operations (claims 10 *et seq.*). It is noted that the purpose of randomly disguising the operation, with a corresponding random disguise of the input data so that the result of performing the disguised operation on the disguised data is the same as if the original operation had been performed on the original data, is to *further* increase the difficulty of determining the nature of the original operation over repeated executions. The Examiner may wonder how a *randomly* disguised operation could achieve the same result as the original operation, the answer being the operations and the input data are randomized in exactly the same way.

The Saada patent, on the other hand, discloses an authenticating method. This has nothing to do with disguising an operation, whether randomly or not. Instead, Saada seeks to verify the authenticity of information I_A sent by sender A to receiver B. The receiver B performs

an operation on a secret set of information shared by the two cards, and checks if received information corresponds to the result obtained using the secret information. It so, then the sender must have possessed corresponding secret information, and the result is authenticated. While the secret data stored in the receiver of Saada might be "disguised," the disguised data is not used in the manner of the claimed invention to disguise an operation *h* that would achieve a result R on undisguised data, by applying a disguised operation h_{R1} on the disguised data. In fact, none of the operations performed by the receiving or sending cards of Saada are disguised, *and the data on which the operations are performed is not even input* data, but rather data already stored in the receiver. The method of Saada merely disguises the secret data on the card. This has nothing to do with the claimed invention, which modifies *input* data in order to disguise operations performed by the card

The data carrier of the claimed invention performs a disguising operation $(x \otimes R_1)$ on input data so that when a disguised (modified) operation h_{R1} is performed on the disguised input data, the result will be the same as if the original operation *h* had been performed on the original data *x*. In contrast, Saada's method involves a receiver and a sender, each of which performs the same operation on the same data to achieve the same result and therefore authentication. This distinction can be illustrated as follows:

Claimed: performed by the operating program of a data carrier chip:

a. $\otimes$ on input data x and random number R_1 to obtain disguised input data;

b. disguised operation $\boldsymbol{h_{R1}}$ performed on disguised input data $\boldsymbol{(x \otimes R_1)}$ so as to obtain a result that equals ***h*** on **input data** without actually performing ***h*** on ***input data***.

Saada: performed by receiver of transmitted data:

a. undisguised operations on secret data S possessed by receiver;

b. undisguised operations on information received from sender;

c. Do results equal each other?; if so received information is authenticated.

Because the Saada patent discloses a method that does not involve all of the steps of the claimed method, and that has an entirely different and unrelated purpose, withdrawal of the rejection of claims 1, 2, 4, 6, 7, 8, and 18 under 35 USC §102(b) is respectfully requested.

4. Rejection of Claims 3, 5, and 9-17 Under 35 USC §103(a) in view of U.S. Patent No. 4,549,075 (Saada) in view of "Applied Cryptography," pp 349-353, 366-367 (Schneier)

This rejection is respectfully traversed on the grounds that the Schneier publication, like the Saada patent, does not disclose or suggest any sort of operating program that varies **(disguises) input data and** an **operation** in such a way that the **outcome** is **unchanged** so as to prevent statistical analysis of signal patterns generated while obtaining a result, as claimed. Instead, the Schneier publication merely discloses that the XOR operation is a known way of protecting data. It does not suggest using the XOR operation to modify input data so that a modified operation can then be performed on the XOR'd input without affecting the result that would have been obtained by performing the original operation on the original data.

The Examiner will note that the present invention does **not seek to protect the input** (although the input could certainly be protected by other means), but rather seeks to **protect the operations** performed by the chip. **Even if the *input* data is originally known, the operations will be protected because both the input data and operation performed thereon are changed (disguised) following input.** The XOR operation is merely one of a number of known ways that could be used to disguise the input data during performance of the disguised operation.

Applying the XOR teachings of Schneier to the authentication method of Saada results, at best, in a modification of the **authentication method** of Schneier in which the secret set of data is protected by XOR instead of the "symmetrical algorithm" J. The result would not have been the claimed invention, and therefore it is respectfully submitted that claims 3, 5, and 9-17 define non-obvious subject matter with respect to the proposed combination of the Saada patent and the Schneier article, whether considered individually or in any reasonable combination. As

a result, withdrawal of the rejection of claims 3, 5, and 9-17 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: September 13, 2004

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\bcu\Pending Q...ZW\WATER 763621\a01.wpd